WRITTEN TESTIMONY OF

JENNIFER BARRETT
CHIEF PRIVACY OFFICER
ACXIOM CORPORATION

BEFORE THE
UNITED STATES HOUSE
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON COMMERCE, TRADE AND CONSUMER PROTECTION

HEARING ON "SECURING CONSUMERS' DATA: OPTIONS FOLLOWING SECURITY BREACHES"

MAY 11, 2005

Summary

Acxiom has an inherent responsibility to safeguard the personal information we collect and bring to the market, and we have focused on assuring the appropriate use of these products and providing a safe environment for this information since 1991 when the company brought its first information products to market.

Information has become an ever growing and ever more integral part of the American economy. Information is the facilitator of convenience and competition, and it provides the tools that reduce fraud and terrorism. As such, we believe that it is Acxiom's obligation to provide effective safeguards to protect the information we bring to market regardless of the difficulties encountered in doing so.

Only Acxiom's fraud management and background screening products involve the transfer of sensitive information. These products, therefore, are subject to law, regulations and our own company policies that help protect against misuse.

> **GLBA and DPPA:** Our fraud management products utilize information covered under the Gramm-Leach-Bliley Act (GLBA), and driver's license information covered under both state and federal driver's privacy protection acts (DPPAs).
>
> **FCRA and FACTA:** Our background screening products are covered by all of the regulations and consumer protections established by the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA).
>
> **Safeguarding Public Record Information:** Although a heightened level of protection is not mandated for public record information, by virtue of the fact that such public information is blended with regulated information, Acxiom *voluntarily chooses* to apply the more stringent standards of the above-mentioned regulations to the resulting products.

Although Acxiom's directory and marketing products do not contain any sensitive information that could put a consumer at risk for identity fraud, Acxiom is still subject to the following critical safeguards: various industry guidelines, compliance with all requirements in the original notice to consumers at the time the data was collected**,** and voluntary compliance with those laws to which our clients themselves are subject.

There has been much discussion, especially in recent weeks, about whether existing federal law sufficiently protects consumers from harm. In this regard, Acxiom does believe that additional, appropriately tailored measures, such as federal preemptive legislation requiring notice to consumers in the event of a security breach, would assist Acxiom, the rest of the information services industry and businesses in general in ensuring that consumers are protected from fraud and identity theft. But, as FTC Chairman Majoras has said, even the best security systems imaginable and the strongest laws possible can nonetheless be circumvented by inventive criminals' intent on committing fraud.

Introduction

Chairman Stearns, Ranking Member Schakowsky and distinguished Members of the Committee, thank you taking the time to hold this hearing on consumer data and options following security breaches. Acxiom appreciates the opportunity to participate in today's hearing.

Acxiom has an inherent responsibility to safeguard the personal information we collect and bring to the market, and we have focused on assuring the appropriate use of these products and providing a safe environment for this information since 1991 when the company brought its first information products to market.

It is important that we all recognize that information has become an ever growing and ever more integral part of the American economy. Information is the facilitator of convenience, competition and provides the tools that reduce fraud and terrorism. As such, we believe that it is Acxiom's obligation to provide effective safeguards to protect the information we bring to market regardless of the difficulties encountered in doing so.

Let me be blunt. The bad guys are smart and getting more organized. They will use all of the skills available to them to try to find ways to obtain the information they need to commit fraud. Acxiom must therefore remain vigilant and innovative, and that is why we employ a world-class information security staff to help us fend off criminals who attempt to access Acxiom's data. Acxiom is constantly improving, auditing and testing its systems. Yes, Acxiom is even learning from security breaches when they occur, and we are certain that other responsible companies are doing so as well.

As Chairman Deborah Majoras of the Federal Trade Commission recently stated in her testimony before the Senate, "[T]here is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." Even though we believe that this is true, no one has a greater interest than Acxiom in protecting information because the company's very existence depends on securing personal information pertaining to consumers.

In order to enjoy the benefits provided by a robust information-based economy and also to keep our citizens safe from fraudulent activity, there are no quick fixes or easy solutions. We believe that it is necessary that cooperation exists among policy makers, information service providers, Acxiom's clients, law enforcement and consumers. We applaud your interest in exploring these issues and we very much want to be a resource in helping you achieve the proper legislative balance we all seek.

About Acxiom Corporation

Founded in 1969, Acxiom is headquartered in Little Rock, Arkansas, with operations throughout the United States, and with processing centers in Arkansas, Illinois, Arizona, Ohio and California. The company also has offices in nine other countries across Europe and Asia. From a small company in Arkansas, Acxiom Corporation has grown into a publicly traded corporation with more than 6,000 employees worldwide

Acxiom's U.S. business includes two distinct components: customized computer services and a line of information products. Acxiom's computer services represent the vast majority of the company's business and they include a wide array of leading technologies and specialized computer services focused on helping clients manage their own customer information. These services are offered exclusively to large businesses, not-for-profit organizations, political parties and candidates, and government agencies. Acxiom's private sector computer services clients represent a "who's who" of America's leading companies. Acxiom helps these clients improve the loyalty of their customers and increase their market share, while reducing risk and assisting them with their compliance responsibilities under state and federal law. Finally, Acxiom helps government agencies improve the accuracy of the personal information they currently hold.

The balance of Acxiom's business comes from information products that are comprised of four categories: fraud management products, background screening products, directory products and marketing products. These four product lines represent less than 20 percent of the company's total business and the fraud management and background screening products represent less than 10 percent. While each product plays a unique role, all of Acxiom's information products help fill an important gap in today's business-to-consumer relationship.

To understand the critical role Acxiom plays in facilitating the nation's economy and safeguarding consumers, it is important to understand what the company *does not* do. Over the years, a number of myths have developed about Acxiom that require clarification. Please allow us to set the record straight:

- Acxiom *does not* maintain one big database that contains detailed information about all individuals. Instead, the company safeguards discrete databases developed and tailored to meet the specific needs of Acxiom's clients – entities that are appropriately screened and with whom Acxiom has legally enforceable contractual commitments. I cannot call up from the company's databases a detailed dossier on myself or any individual.

- Acxiom *does not* provide information on particular individuals to the public, with the exception of Acxiom's telephone directory products. These products, which are available on several Internet search engines, contain information already available to the public. The other information Acxiom processes is provided only to legitimate businesses for specific legitimate business purposes.

- Acxiom's *does not* have any information in either its directory or marketing products which could be used to commit identity fraud. Acxiom also *does not* include detailed or specific transaction-related information, such as what purchases an individual made on the Internet or what websites they visited. The company's directory products include only name, address and telephone information. The company's marketing products include only information that is general in nature and not specific to an individual purchase or transaction.

- Acxiom *does not* commingle client information that the company processes in its computer services business with any of our information products. Such activity would constitute a violation of the company's services contracts with those clients and a violation of consumer privacy. A client for whom the company performs services may have a different agreement with us as a data contributor, but these two relationships are kept entirely separate.

Acxiom's fraud management products are sold exclusively to a handful of large companies and government agencies – they are not sold to individuals. The company's verification services only validate that the information our client has obtained from the consumer is correct. Only law enforcement, government agencies and the internal fraud departments of large financial institutions and insurance companies have access to additional information.

Acxiom's background screening products provide employment and tenant screening services which utilize field researchers who do in-person, real-time research against public records and make calls to past employers to verify the information provided by the consumer. Where permitted by law, a pre-employment credit report can also be obtained. Acxiom does not pre-aggregate information for these products.

Acxiom's directory information products contain only contact information on consumers such as name, address and telephone number. They are collected so businesses and consumers can locate other businesses or consumers. They are compiled from the white and yellow pages of published U.S. and Canadian telephone directories and from information available from the various directory assistance services provided by the telephone companies.

Acxiom's marketing information products provide demographic, lifestyle and interest information to companies to reach prospective new customers who are most likely to have an interest in their products and to better understand and serve the needs of existing customers. They are compiled from pubic records, surveys and summarized customer information primarily from publishers and catalogers.

Respecting and Protecting Consumers' Privacy

Acxiom has a longstanding tradition and engrained culture of protecting and respecting consumer interests in our business. The company is today, and always has been, a leader in developing self-regulatory guidelines and in establishing security policies and privacy practices. There are, as explained below, numerous laws and regulations that govern our business. Ultimately, however, Acxiom's own comprehensive approach to information use and security goes far beyond what is required by either law or self-regulation.

Safeguards Applicable to Products Involving the Transfer of Sensitive Information

Only Acxiom's fraud management and background screening products involve the transfer of sensitive information. These products, therefore, are subject to law,

regulations and our own company policies that help protect against identity fraud. These legal protections and additional safeguards are addressed below:

GLBA, DPPAs, and FTC: Our fraud management products utilize information covered under the Gramm-Leach-Bliley Act (GLBA), and driver's license information covered under both state and federal driver's privacy protection acts (DPPAs). These obligations include honoring GLBA and DPPA notice and choice related to sharing and use of the information, the GLBA Safeguard Rules and FTC Privacy Rule and Interagency Guidelines. Any uses of data must fall within one of the permitted uses or exceptions specified in these laws.

FCRA and FACTA: Our background screening products are covered by all of the regulations and consumer protections established by the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA). These protections include: the requirement that a consumer authorize the creation of employment reports; notice of adverse actions taken based on such report; and the right of consumers to obtain a copy of such reports and to dispute inaccuracies. Finally, such regulations require that re-verification or correction of disputed information be performed in a timely manner.

Safeguarding Public Record Information: Public records are used in both Acxiom's fraud management and background screening products. Although a heightened level of protection is not mandated for such public record information, by virtue of the fact that such public information is blended with regulated information, Acxiom *voluntarily chooses* to apply the more stringent standards of the above-mentioned regulations to the resulting products.

Safeguards Applicable to Other Products

Although Acxiom's directory and marketing products do not contain any sensitive information that could put a consumer at risk for identity fraud, Acxiom is still subject to the following critical safeguards: various industry guidelines, compliance with all requirements in the original notice to consumers at the time the data was collected**,** and voluntary compliance with those laws to which our clients themselves are subject.

Telephone Directory Safeguards: Acxiom's directory products comply with all applicable policies regarding unpublished and unlisted telephone numbers and addresses. In addition, because Acxiom recognizes that consumers may object to published listings being available on the Internet, Acxiom *itself* offers an opt-out from such use. Further, Acxiom voluntarily suppresses all telephone numbers found on the Federal Trade Commission's Do-Not-Call Registry and the eleven other state Do-Not-Call registries, when providing phone numbers for targeted telemarketing purposes.

Marketing Product Safeguards: Acxiom's marketing products comply with all the self-regulatory guidelines issued by the Direct Marketing Association. These requirements include notice and the opportunity to opt-out. Consumers have the ability to opt-out from Acxiom's marketing products by calling the company's

toll-free Consumer Hotline, accessing its Website, or by writing to the company. Since Acxiom does not have a customer relationship with individual consumers, Acxiom coordinates with its industry clients to research and resolve consumer inquiries.

Additional Safeguards

Acxiom takes seriously its responsibility to assure that all the information we bring to market is appropriate for the use to which it is intended and to provide adequate safeguards specifically aimed at protecting against unauthorized use.

Privacy Policy / FTC Jurisdiction: Since 1997, long before it was a common practice, Acxiom has posted its privacy policy on the company's website. The privacy policy describes both Acxiom's online and offline consumer information products. The policy further describes: what data Acxiom collects for these products; how such data is used; the types of clients to which such data is licensed; as well as the choices available to consumers as to how such data is used. By making these extensive disclosures, Acxiom has voluntarily subjected itself to Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive conduct in the course of trade or commerce, as well as various state statutes governing unfair and deceptive acts and practices.

Consumer Care Department / Consumer Hotline: Acxiom maintains a Consumer Care Department led by a Consumer Advocate whose team interacted with more than 50,000 consumers in the past 12 months by way of answering questions, resolving issues, processing opt-outs, and handling requests for access to Acxiom's fraud management, background screening, directory and marketing products. Acxiom provides consumers who contact the company (through the company website, or by calling a toll-free Consumer Hotline or by writing to the company) the options of: opting-out of all of Acxiom's marketing products; receiving an information report from the company's fraud management and directory products; or receiving a consumer report as specified in the FCRA from the company's background screening products. Acxiom encourages consumers to notify the company if the information in any of these reports is inaccurate and it is the company's policy either to correct the information, to delete it or to refer the consumer to the appropriate source to obtain the requested correction, such as a county or state agency.

Certification and Compliance with Federal and State Law: Acxiom's privacy policy is designed to adhere to all Federal, State, and local laws and regulations on the use of personal information. The company is also certified under the Department of Commerce's European Union Safe Harbor and the Better Business Bureau's Online Seal.

Consumer Education: Acxiom believes that consumers should be educated about how businesses use information. To that end, Acxiom publishes a booklet, entitled "*Protecting Your Privacy in the Information Age - What Every Consumer*

Should Know About the Use of Individual Information," which is available for free both on the company's website and upon written or telephone request.

Voluntary Acxiom Policies: Above and beyond the industry-accepted guidelines with which Acxiom complies, Acxiom also has established its own internal guidelines, which are more restrictive than industry standards. For example, Acxiom only collects the specific information required to meet its clients' information needs, and the company properly disposes of the remaining data, when information is compiled from public records. Acxiom has also implemented specific guidelines regarding the use and protection of information that could be involved in identity fraud, such as Social Security numbers.

Information Practice and Security Audits: Acxiom has had a longstanding focus on the appropriate use of information in developing and delivering its information products. While the creation of strong information use policies is a business imperative, assuring these policies are followed is equally important. To this end, all of Acxiom's information products and practices have been internally and externally audited on an annual basis since 1997.

Since many of Acxiom's computer service clients are financial institutions and insurance agencies, Acxiom has been regularly audited for many years by these clients. Furthermore, Acxiom must honor the safeguards and security policies of the company's clients. Since Acxiom's security program is enterprise-wide, it is the company's policy to institute these high levels of protection across all lines of business. These client audits, along with Acxiom's own internal security audits, provide Acxiom with regular and valuable feedback on ways to stay ahead of hackers and fraudsters who may attempt to gain unauthorized access to Acxiom's systems.

Lessons Learned

Two years ago, Acxiom experienced a security breach on one of the company's external file transfer servers. The hackers were employees of an Acxiom client and a client's contractor. As users with legitimate access to the server, the hackers had received authority to transfer and receive their own files. The hackers did not penetrate the firewalls to Acxiom's main system. They did, however, exceed their authority when they accessed an encrypted password file on the server and successfully unencrypted about 10 percent of the passwords, which allowed them to gain access to other client files on the server. Fortunately, the vast majority of the information involved in this incident was of a non-sensitive nature.

Upon learning of the initial breach from law enforcement, Acxiom immediately notified all affected clients and, upon further forensic investigation, the company informed law enforcement regarding a second suspected security incident. Fortunately, in both instances, law enforcement was able to apprehend the suspects, recover the affected information and ascertain that none of the information was used to commit identity fraud.

One of the hackers pled guilty and was recently sentenced to 48 months in federal prison. The other is currently awaiting trial.

As a result of the breach, Acxiom cooperated with audits conducted by dozens of its clients, and both the Federal Trade Commission and the Office of the Comptroller of the Currency examined Acxiom's processes to ensure that the company was in compliance with all applicable laws and its own stated policies.

This experience taught Acxiom additional valuable lessons regarding the protection of information. For example, Acxiom now requires the use of more secure passwords on the affected server. The process for transferring files has been changed, specifically by keeping information on the server for much shorter periods of time. And while it was always a recommended internal policy, Acxiom now requires that all sensitive information passed across such servers be encrypted. In addition, while Acxiom has had in place a Security Oversight Committee for many years, the company has also now appointed a Chief Security Officer with more than 20 years of IT experience. In short, Acxiom's systems are more secure today as a result of the company's experience and dedication to the privacy of consumers.

The Need For Additional Legislative Safeguards

There has been much discussion, especially in recent weeks, about whether existing federal law sufficiently protects consumers from harm. In this regard, Acxiom does believe that additional, appropriately tailored legislation would assist Acxiom, the rest of the information services industry and businesses in general in ensuring that consumers are protected from fraud and identity theft. But, as FTC Chairman Majoras has said, even the best security systems imaginable and the strongest laws possible can nonetheless be circumvented by inventive criminals' intent on committing fraud.

Breach Notification: Acxiom supports efforts to pass federal preemptive legislation requiring notice to consumers in the event of a security breach, where such breach places consumers at risk of identity theft or fraud. California implemented similar legislation several years ago, and over thirty other states are involved in passing similar laws. The bottom line is that consumers deserve a nationwide mandate that requires that they be notified when they are at risk of identity theft, so they can take appropriate steps to protect themselves.

Extension of the GLBA Safeguards Rule: Currently, Acxiom voluntarily subjects itself to the GLBA Safeguards Rule with respect to the company's computer services and information products. Acxiom also complies with the California safeguards law (AB 1950). FTC Chairman Majoras recently has proposed an extension of the GLBA Safeguards Rule to the information services industry as a whole. Acxiom supports her recommendation.

Mr. Chairman, Acxiom appreciates the opportunity to participate in this hearing and to assist Congress in identifying how best to safeguard the nation's information and data. Acxiom is available to provide any additional information the Committee may request.